DIPLOMADO DE PROFUNDIZACIÓN CISCO, DISEÑO E IMPLEMENTACION DE SOLUCIONES INTEGRADAS LAN / WLAN

PRUEBA DE HABILIDADES PRÁCTICAS

PRESENTADO POR

LIEVER ROJAS SCARPETA

PRESENTADO A

NILSON ALBEIRO FERREIRA MANZANARES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA

PITALITO - HUILA

2020

Tabla de contenido

Resumen

El propósito principal de este contenido es dar a conocer los resultados obtenidos durante el desarrollo de los diferentes trabajos colaborativos que se abordaron y solucionaron durante el curso, lo importante es dar a conocer que contamos con capacidades para resolver problemas de redes dentro de una empresa o para empezar a trabajar como independientes.

La Universidad Nacional Abierta y a Distancia UNAD en colaboración con CISCO Networking Academy ha puesto en marcha el diplomado CISCO diseño e implementación de redes LAN-WAN como opción de grado para los estudiantes que están culminando sus estudios en ingeniería de sistemas, aparte de la gran facilidad de opción de grado es un curso que nos brinda una gran cantidad de recursos y conocimientos para adentrarnos en un mundo de redes de forma profesional.

Abstract

The main purpose of this content is to publicize the results obtained during the development of the different collaborative works that are addressed and resolved during the course, the important thing is to make known that we have capabilities to solve network problems within a company or in To start working as freelancers.

The National Open and Distance University UNAD in collaboration with CISCO Networking Academy has launched the CISCO diploma design and implementation of LAN-WAN networks as a degree option for students who are completing their studies in systems engineering, apart from the great ease The degree option is a course that gives us a lot of resources and knowledge to enter a world of networks in a professional way.

Introducción

La globalización de internet ha producido un cambio significativo en el crecimiento y en cómo se comunican las empresas de tecnología, ya que ninguna quiere quedarse fuera de este constante desarrollo tecnológico. A medida que programadores y especialistas en TI evolucionen en crear cada vez lo imposible en el ámbito de las comunicaciones, las empresas seguirán su ritmo o si no desaparecerán.

Hoy día el funcionamiento de una empresa consta de muchos factores importantes entre uno de ellos está el de la red, este es de mucha importancia para poder realizar la comunicación con todos los canales que esta cuenta y para ellos debemos conocer cómo funciona y como se debe implementar ya sea en una casa, une pequeña empresa o una gran corporación.

En estos documentos vamos a mostrar algunas cosas especiales de cómo se debe configurara e implementar. Para resolver este caso de estudio es necesario implementar configuración de enrutamiento, asignar direcciones Ip, configuración de protocolos de enrutamiento y diseñar e implementar NAT estáticas.

Objetivo General

Desarrollar el caso de estudio CCNA de la prueba de habilidades prácticas que forma parte de las actividades evaluativas del Diplomado de Profundización CCNA, la cual busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado y a través de la cual se pondrá a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

1. Escenario uno

Una empresa posee sucursales distribuidas en las ciudades de Bogotá, Medellín y Cali en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

1. Topología de red

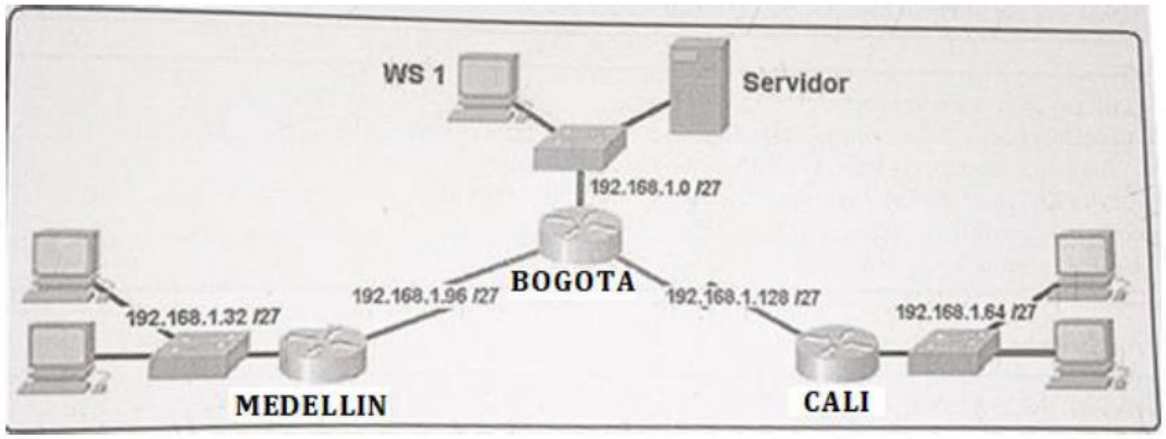

Figura 1. Imagen de topología tomada de red inicial para el escenario

1.1 Topología de red en Packet Tracer

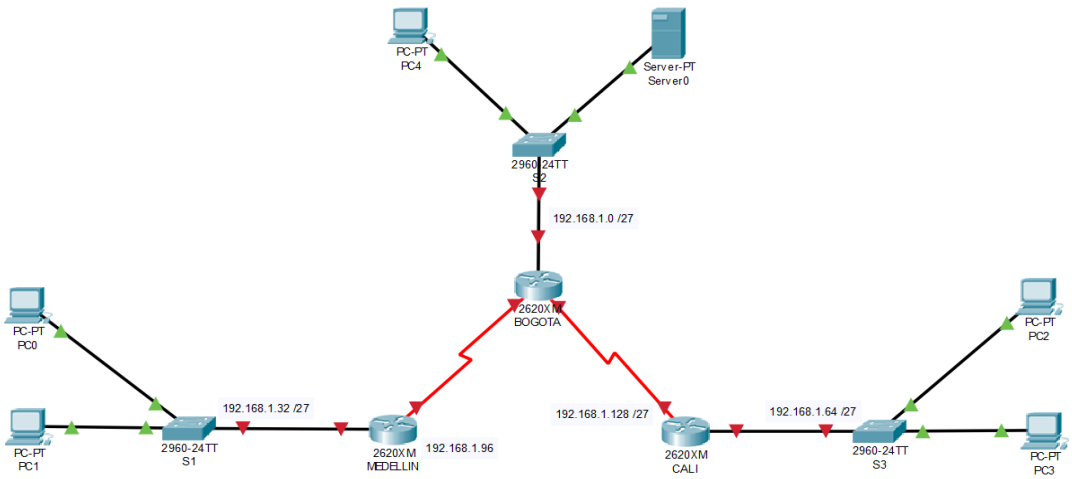

Figura 2. Imagen de topología en Packet Tracer

1.2 Tabla de enrutamiento para la red

	R1	R2	R3
Nombre de Host	MEDELLIN	BOGOTA	CALI
Dirección de Ip en interfaz Serial 0/0	192.168.1.99	192.168.1.98	192.168.1.131
Dirección de Ip en interfaz Serial 0/1		192.168.1.130	
Dirección de Ip en interfaz FA 0/0	192.168.1.33	192.168.1.1	192.168.1.65
Protocolo de enrutamiento	Eigrp	Eigrp	Eigrp
Sistema Autónomo	200	200	200
Afirmaciones de red	192.168.1.0	192.168.1.0	192.168.1.0

Tabla 1. Tabla de configuración de dispositivos

1.3 Configuración inicial de dispositivos

1.3.1 Router Bogotá

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lo
Router(config)#no ip domain-lookup
Router(config)#Hostname BOGOTA
BOGOTA(config)#enable secret cisco
BOGOTA(config)#line console 0
BOGOTA(config-line)#password cisco
BOGOTA (config-line)#login
BOGOTA(config-line)#exit
BOGOTA(config)#line vty 0 4
BOGOTA(config-line)#password cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#exit
BOGOTA(config)#service password-encryption
BOGOTA(config)#banner motd #Acceso solo a personal autorizado#
BOGOTA(config)#exit
BOGOTA#
%SYS-5-CONFIG_I: Configured from console by console
BOGOTA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
BOGOTA#
```

1.3.2 Router Medellín

```
Router>enable
Router#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname MEDELLIN
MEDELLIN(config)#enable secret cisco
MEDELLIN(config)#line console 0
MEDELLIN(config-line)#password cisco
MEDELLIN(config-line)#login
MEDELLIN(config-line)#exit
MEDELLIN(config)#line vty 0 4
MEDELLIN(config-line)#password cisco
MEDELLIN(config-line)#login
MEDELLIN(config-line)#exit
MEDELLIN(config)#service password-encryption
MEDELLIN(config)#banner motd #Acceso solo a personal autorizado#
MEDELLIN(config)#exit
MEDELLIN#
%SYS-5-CONFIG_I: Configured from console by console
MEDELLIN#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
MEDELLIN#
```

1.3.3 Router Cali

```
Router>enable
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname CALI
CALI(config)#enable secret cisco
CALI(config)#line console 0
CALI(config-line)#password cisco
CALI(config-line)#login
CALI(config-line)#exit
CALI(config)#line vty 0 4
CALI(config-line)#password cisco
CALI(config-line)#login
CALI(config-line)#exit
CALI(config)#service password-encryption
CALI(config)#banner motd #Acceso solo a personal autorizado#
```

```
CALI(config)#exit
CALI#
%SYS-5-CONFIG_I: Configured from console by console
CALI#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
CALI#
```

1.3.4 **Switch** S1

```
Switch>enable
Switch#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#enable secret cisco
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#service password-encryption
S1(config)#banner motd #Acceso solo a personal autorizado#
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

1.3.5 Switch S2

```
Switch>enable
Switch#conf termi
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#enable secret cisco
S2(config)#line console 0
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#exit
```

```
S2(config)#line vty 0 4
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#service password-encryption
S2(config)#banner motd #Acceso solo a personal autorizado#
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console
S2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S2#
```

1.3.6 Switch S3

```
Switch>enable
Switch#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S3
S3(config)#enable secret cisco
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#line vty 0 4
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#service password-encryption
S3(config)#banner motd #Acceso solo a personal autorizado#
S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console
S3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S3#
```

1.4 Configuración interfaz y seriales

Se realizó la configuración de las interfaces y los seriales según se estableció en la tabla para el escenario uno.

1.4.1 Router Bogotá

```
Acceso solo a personal autorizado
User Access Verification
Password:
BOGOTA>enable
Password:
BOGOTA#conf term
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#interface fastethernet 0/0
BOGOTA(config-if)#ip address 192.168.1.1 255.255.255.224
BOGOTA(config-if)#no shutdown
BOGOTA(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up
BOGOTA(config-if)#exit
BOGOTA(config)#interface serial 0/0
BOGOTA(config-if)#ip address 192.168.1.98 255.255.255.224
BOGOTA(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0, changed state to down
BOGOTA(config-if)#exit
BOGOTA(config)#interface serial 0/1
BOGOTA(config-if)#ip address 192.168.1.130 255.255.255.224
BOGOTA(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1, changed state to down
BOGOTA(config-if)#exit
BOGOTA(config)#ip route 192.168.1.64 255.255.255.224 192.168.1.131
BOGOTA(config)#ip route 192.168.1.32 255.255.255.224 192.168.1.99
BOGOTA(config)#exit
BOGOTA#
%SYS-5-CONFIG_I: Configured from console by console
BOGOTA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
BOGOTA#
```

1.4.2 Router Medellín

```
Acceso solo a personal autorizado
User Access Verification
Password:

MEDELLIN>enable
Password:
MEDELLIN#conf term
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#interface fastEthernet 0/0
MEDELLIN(config-if)#ip address 192.168.1.33 255.255.255.224
MEDELLIN(config-if)#no shutdown
MEDELLIN(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up
MEDELLIN(config-if)#exit
MEDELLIN(config)#interface serial 0/0
MEDELLIN(config-if)#ip address 192.168.1.99 255.255.255.224
MEDELLIN(config-if)#no shutdown
MEDELLIN(config-if)#
%LINK-5-CHANGED: Interface Serial0/0, changed state to up
MEDELLIN(config-if)#exit
MEDELLIN(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to
up
ip route 192.168.1.0 255.255.255.224 192.168.1.97
MEDELLIN(config)#ip route 192.168.1.0 255.255.255.224 192.168.1.97
MEDELLIN(config)#ip route 192.168.1.64 255.255.255.224 192.168.1.97
MEDELLIN(config)#exit
MEDELLIN#
%SYS-5-CONFIG_I: Configured from console by console
MEDELLIN#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
MEDELLIN#
```

1.4.3 Router Cali

```
Acceso solo a personal autorizado
User Access Verification
Password:
CALI>enable
Password:
CALI#conf term
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#interface fastethernet 0/0
CALI(config-if)#ip address 192.168.1.65 255.255.255.224
CALI(config-if)#no shutdown
CALI(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up
CALI(config-if)#exit
CALI(config)#interface serial 0/0
CALI(config-if)#ip address 192.168.1.131 255.255.255.224
CALI(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0, changed state to down
CALI(config-if)#
CALI(config-if)#exit
CALI(config)#ip route 192.168.1.0 255.255.255.224 192.168.1.129
CALI(config)#ip route 192.168.1.32 255.255.255.224 192.168.1.129
CALI(config)#exit
CALI#
%SYS-5-CONFIG_I: Configured from console by console
CALI#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
CALI#
```

1.5 Verificación de la tabla enrutamientos en los Router

Se procede a la verificación de los Router dependiendo de su tabla de enrutamiento

1.5.1 Router Bogotá

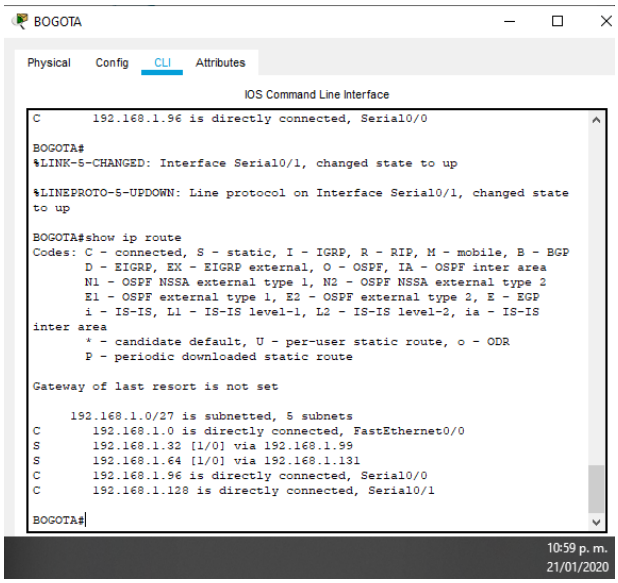

Figura 3. Imagen router Bogotá

1.5.2 Router Medellín

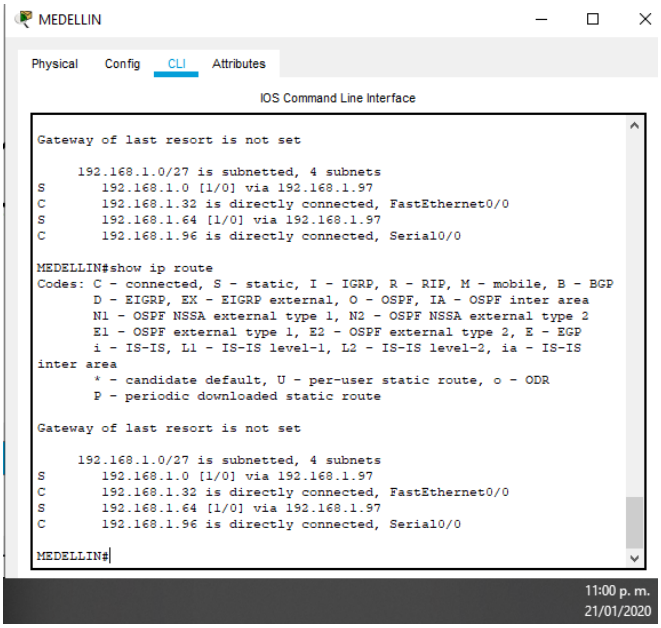

Figura 4. Imagen router Medellín

1.5.3 Router Cali

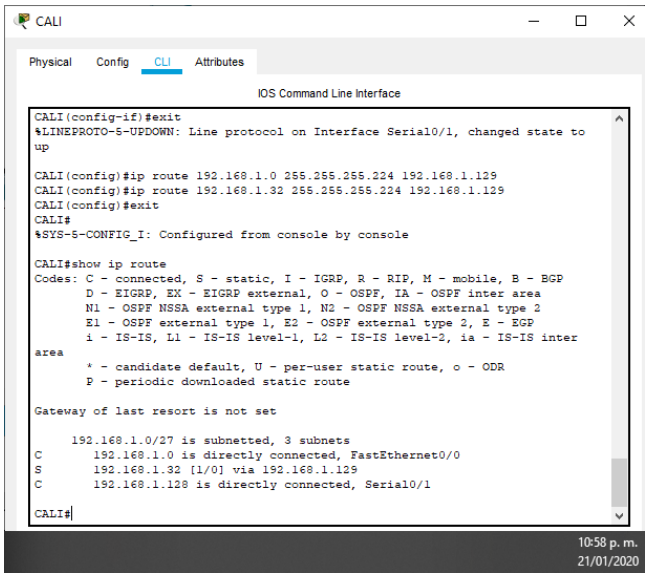

Figura 5. Imagen router Cali

1.6 Verificación balance de Vargas en los routers

El balance de carga se designa mediante el comando ip route, y es dado para los routers que tienen dos seriales conectados.

1.6.1 Router Bogotá

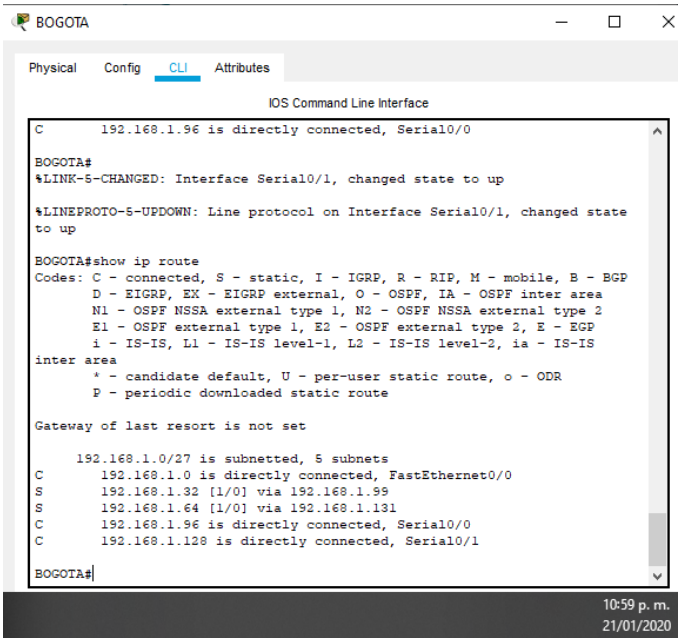

Figura 6. Imagen router Bogotá

1.6.2 Router Medellín

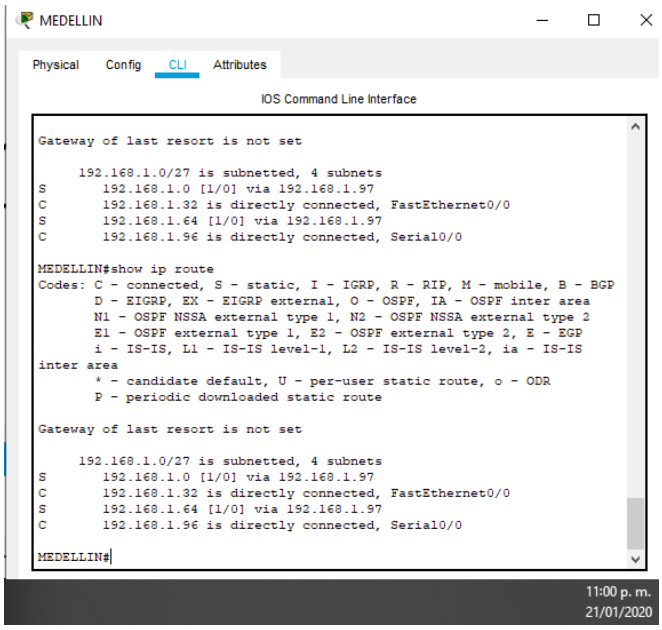

Figura 7. Imagen router Medellín

1.6.3 Router Cali

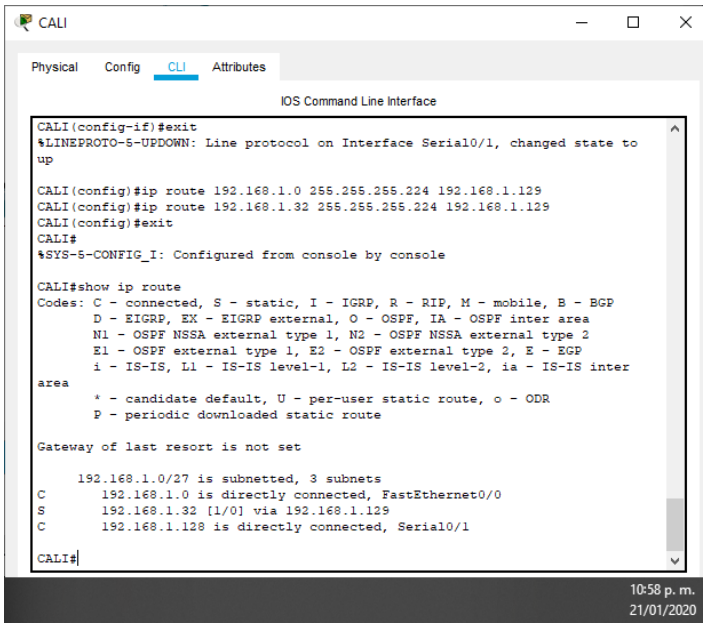

Figura 8. Imagen router Cali

1.7 Verificación de vecinos usando el comando cdp

La verificación de vecinos se utiliza bajo el comando show cdp neighbors, en cada uno de los routers

1.7.1 Router Bogotá

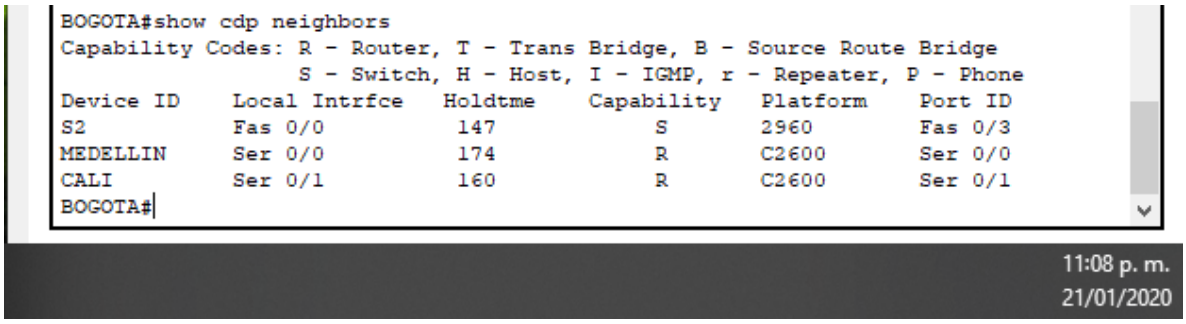

Figura 7. Imagen router Bogotá

1.7.2 Router Medellín

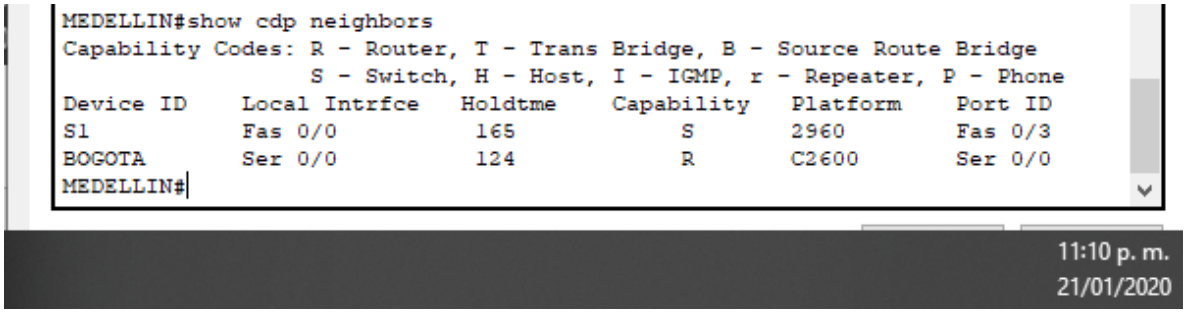

Figura 8. Imagen router Medellín

1.7.3 Router Cali

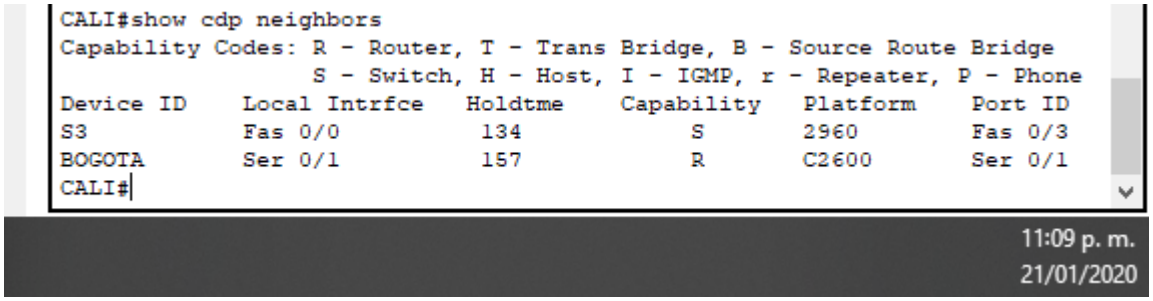

Figura 7. Imagen router Cali

1.8 Asignación de enrutamiento EIGRP

Se realiza la asignación de enrutamiento EIGRP a los routers considerando el direccionamiento diseñado.

1.8.1 Router Bogotá

```
BOGOTA>enable
Password:
BOGOTA#conf term
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#router eigrp 10
BOGOTA(config-router)#network 192.168.1.0 0.0.0.31
BOGOTA(config-router)#network 192.168.1.96 0.0.0.31
BOGOTA(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 192.168.1.99 (Serial0/0) is up:
new adjacency
BOGOTA(config-router)#network 192.168.1.128 0.0.0.31
BOGOTA(config-router)#no auto-summary
BOGOTA(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 192.168.1.99 (Serial0/0) resync:
summary configured
BOGOTA(config-router)#exit
BOGOTA(config)#
```

1.8.2 Router Medellín

```
MEDELLIN>enable
Password:
MEDELLIN#conf term
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#router eigrp 10
MEDELLIN(config-router)#network 192.168.1.96 0.0.0.31
MEDELLIN(config-router)#network 192.168.1.32 0.0.0.31
MEDELLIN(config-router)#network 192.168.1.128 0.0.0.31
MEDELLIN(config-router)#
```

1.8.3 Router Cali

CALI>enable
Password:
CALI#conf term
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#router eigrp 10
CALI(config-router)#network 192.168.1.128 0.0.0.31
CALI(config-router)#network 192.168.1.64 0.0.0.31
CALI(config-router)#no auto-summary
CALI(config-router)#exit
CALI(config)#exit

1.9 Verificación de vecindad EIGRP en los routers

Se realiza la verificación de vecindad dada por los comandos show ip eigrp neighbors y show ip eigrp topology

1.9.1 Router Bogotá

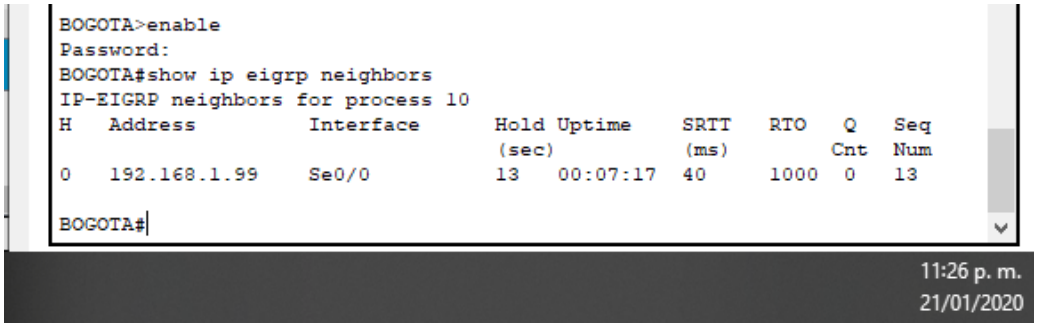

Figura 10. Imagen router Bogotá

1.9.2 Router Medellín

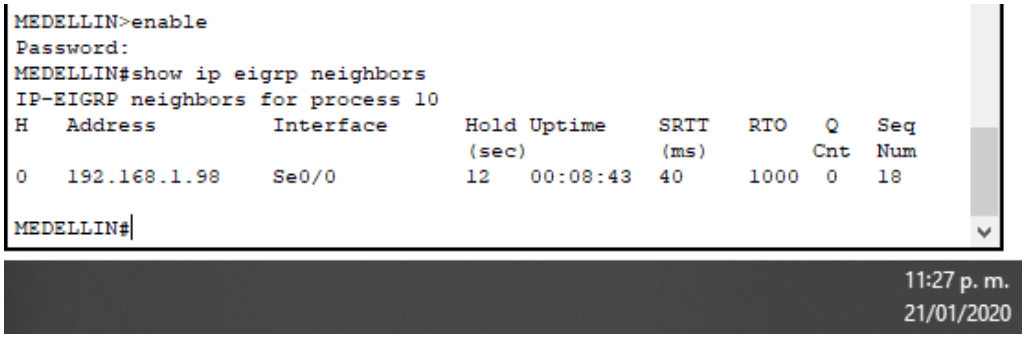

Figura 11. Imagen router Medellín

1.9.3 Router Cali

```
CALI#show ip eigrp neighbors
IP-EIGRP neighbors for process 10
H   Address         Interface       Hold Uptime    SRTT   RTO   Q
Seq
                                    (sec)          (ms)       Cnt
Num
0   192.168.1.130   Se0/0           11   00:12:28  40     1000  0   25

CALI#
```

Figura 12. Imagen router Cali

1.10 Comprobación en las tablas de enrutamientos

Se comprueba mediante el comando show ip route

1.10.1 Router Bogotá

```
BOGOTA#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.1.0/27 is subnetted, 5 subnets
C       192.168.1.0 is directly connected, FastEthernet0/0
S       192.168.1.32 [1/0] via 192.168.1.99
S       192.168.1.64 [1/0] via 192.168.1.131
C       192.168.1.96 is directly connected, Serial0/0
C       192.168.1.128 is directly connected, Serial0/1

BOGOTA#
```

11:37 p. m.
21/01/2020

Figura 13. Imagen router Bogotá

1.10.2 Router Medellín

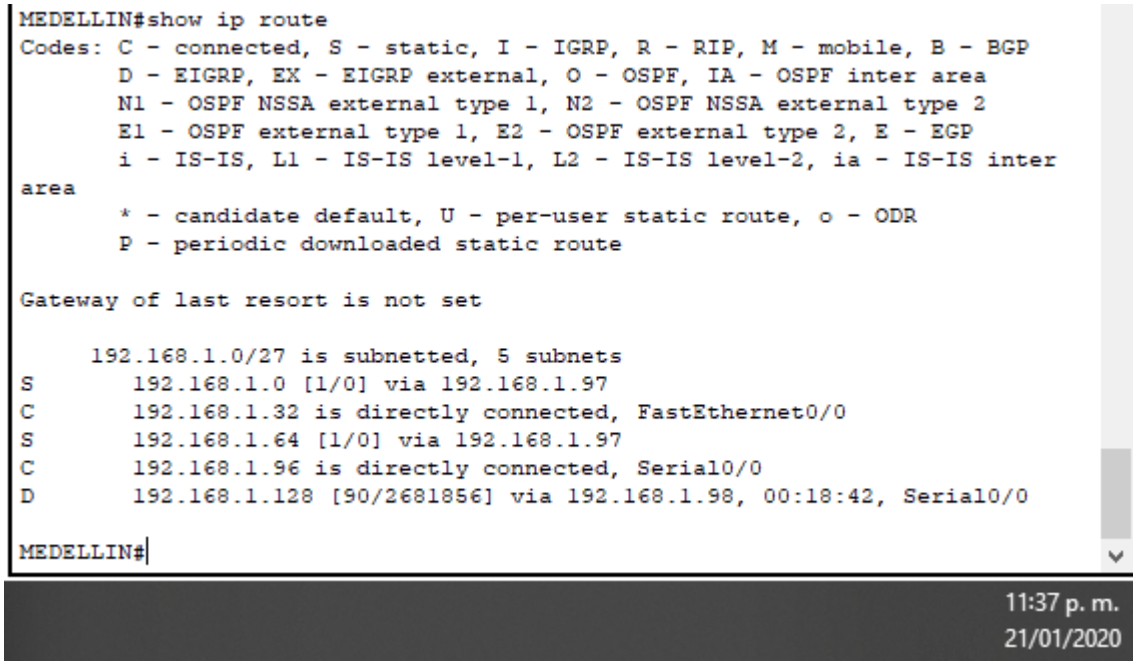

Figura 14. Imagen router Medellín

1.10.3 Router Cali

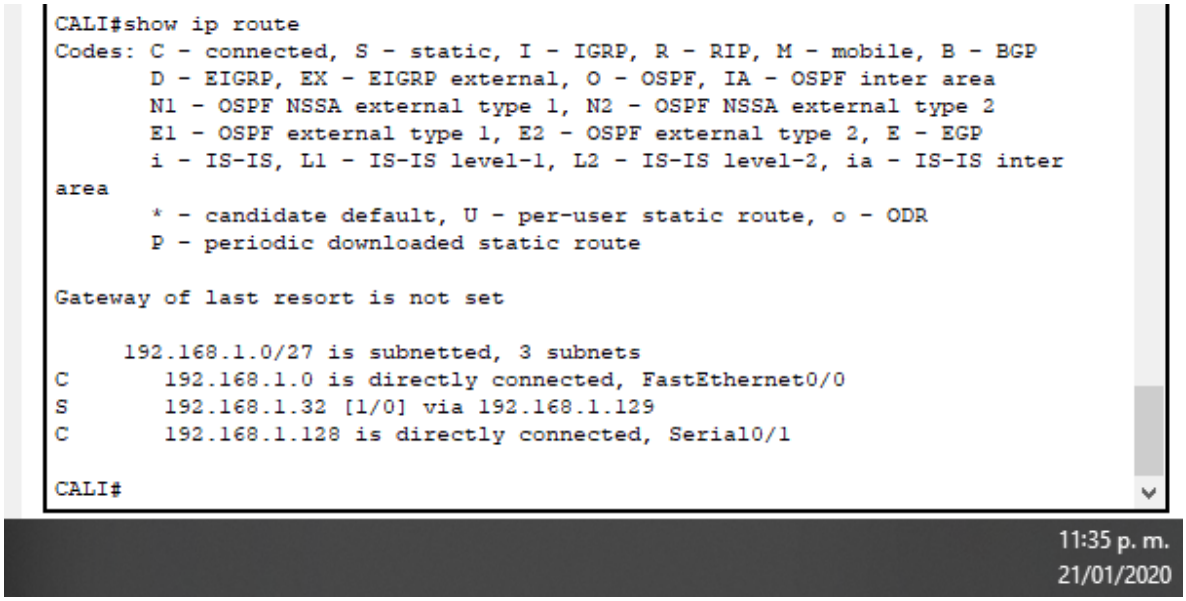

Figura 15. Imagen router Cali

1.11 Diagnóstico de comprobación de puntos de la red

Se realiza comprobación de diagnostico mediante el comando ping para verificar los puntos de Red del escenario.

1.11.1 Host de red LAN del router Cali a red Medellín

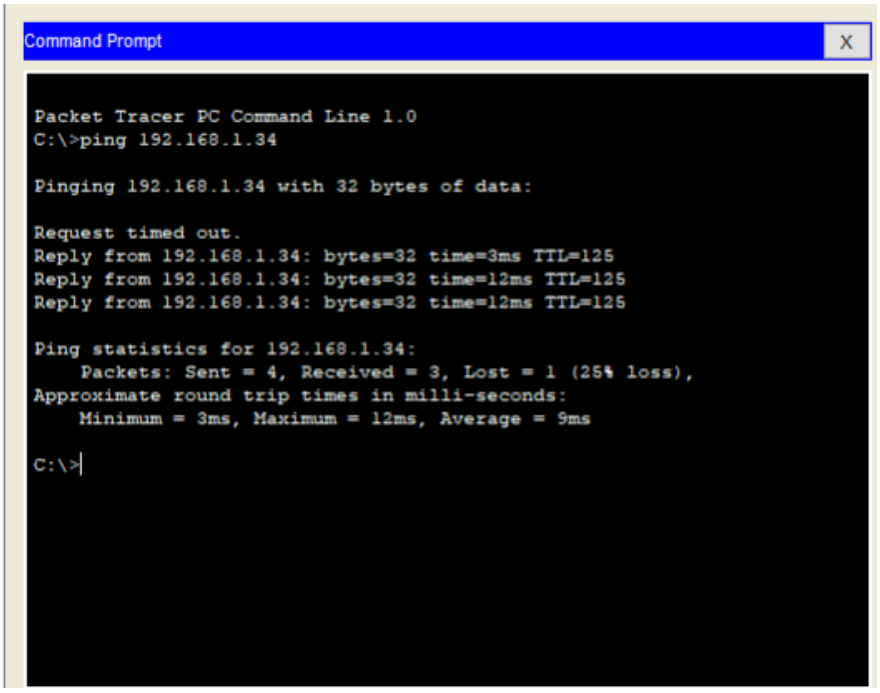

Figura 16. Imagnes ping de LAN Cali a red Medellin

1.11.2 Host de red LAN del router Cali a red servidor

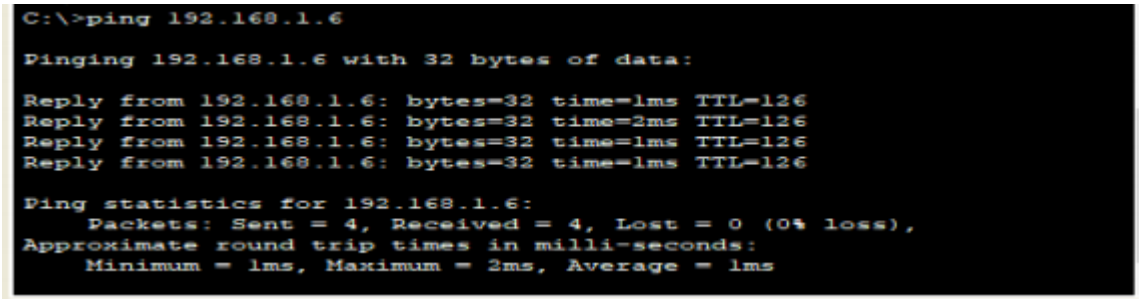

Figura 17. Imágenes ping de LAN Cali a red Servidor

1.12 Configuración list de control de acceso

En este momento cualquier usuario de la Red tiene acceso a todos sus dispositivos y estaciones de trabajo. El jefe de redes le solicita implementar seguridad en la red. Para esta labor se decide configurar listas de control de acceso (ACL) a los routers. Las condiciones para crear las ACL son las siguientes:

Configuración de habilitación para establecer conexións Telnet.

En la configuración inicial de cada routes se establecio la configuración necesaria para la habilitacion de la conexiónes Telnet.

1.12.1 Router Bogotá

```
BOGOTA>enable
Password:
BOGOTA#confi
BOGOTA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#line vty 0 4
BOGOTA(config-line)#password cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#exit
BOGOTA(config)#
```

1.12.2 Router Medellín

```
MEDELLIN#conf term
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#line vty 0 4
MEDELLIN(config-line)#password cisco
MEDELLIN(config-line)#login
MEDELLIN(config-line)#exit
MEDELLIN(config)#
```

1.12.3 Router Cali

```
CALI#conf term
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#line vty 0 15
CALI(config-line)#password cisco
CALI(config-line)#login
CALI(config-line)#exit
```

1.12.4 Conexión Telnet entre routers Medellin-Bogota

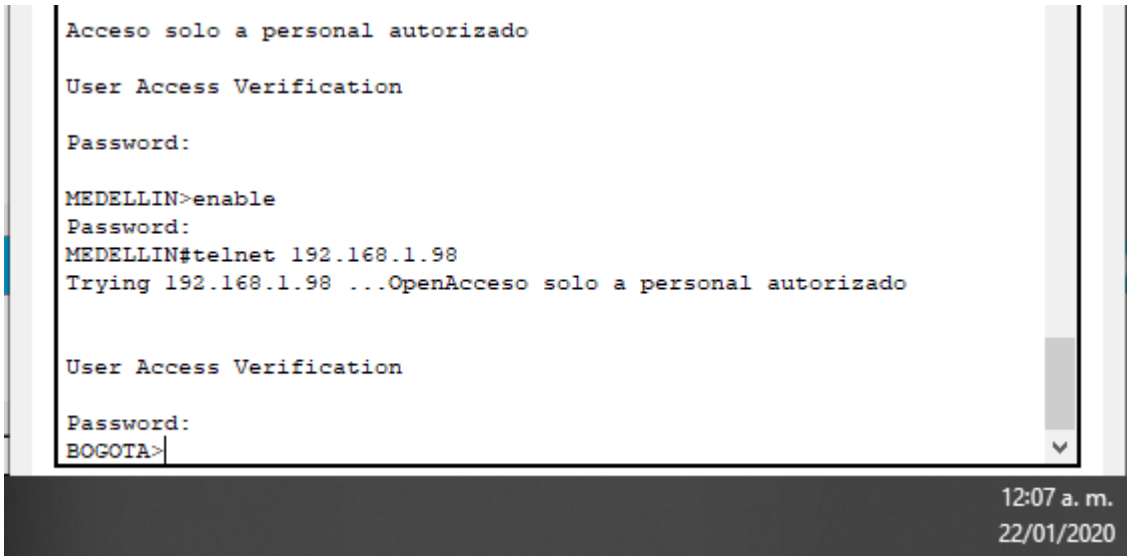

Figura 17. Imagen router entre Medellín y Bogotá

1.12.5 Conexión Telnet entre routers Cali-Bogota

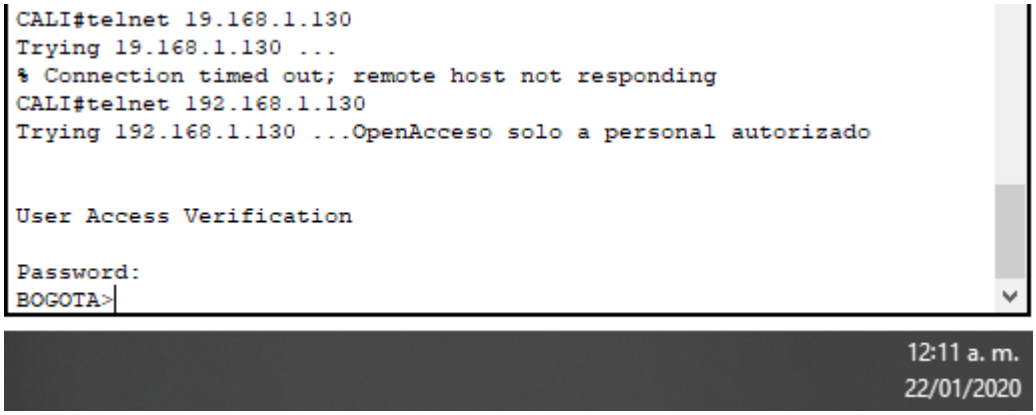

Figura 18. Imagen router entre Cali y Bogotá

1.12.6 Conexión Telnet entre routers Bogotá . Medellín/Cali

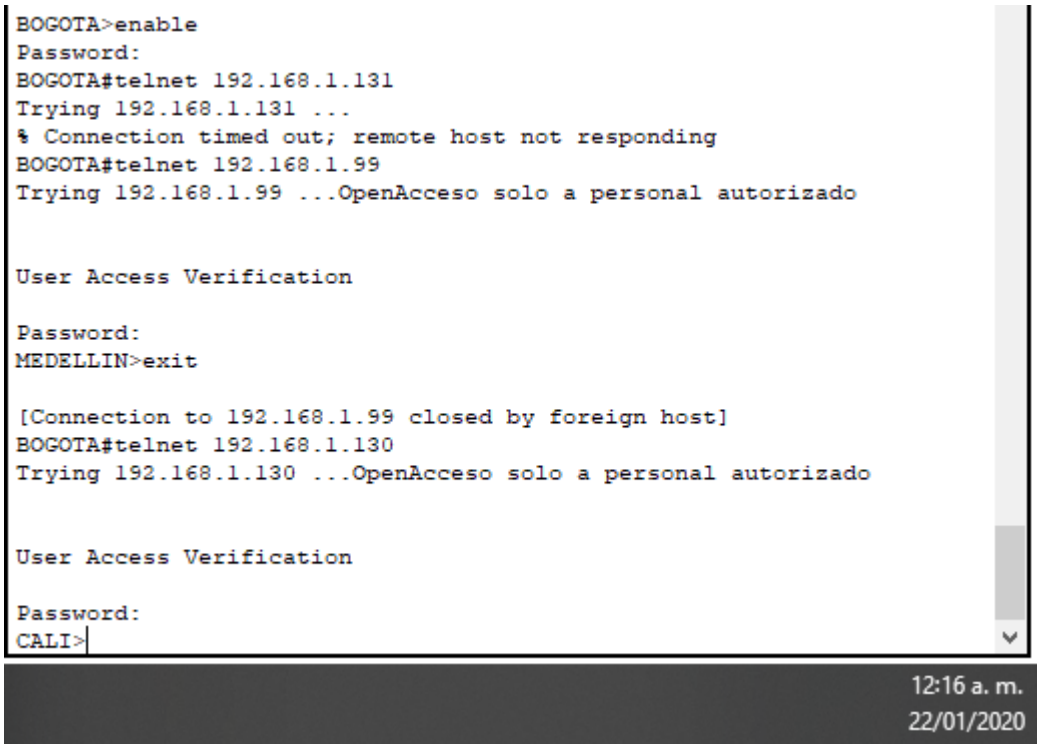

Figura 19. Imagen router entre Bogota y Medellín/Cali

El equipo WS1 y el servidor se encuentran en la subred de administración. Solo el servidor de la subred de administración debe tener acceso a cualquier otro dispositivo en cualquier parte de la red.

BOGOTA#conf term
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#access-list 1 permit 192.168.1.6 0.0.0.224
BOGOTA(config)#access-list 1 deny any
BOGOTA(config)#int se0/0
BOGOTA(config-if)#ip access-group 1 out
BOGOTA(config-if)#exit
BOGOTA(config)#int se0/1
BOGOTA(config-if)#ip access-group 1 out
BOGOTA(config-if)#exit
BOGOTA(config)#exit
BOGOTA#

a. Las estaciones de trabajo en las LAN de MEDELLIN y CALI no deben tener acceso a ningún dispositivo fuera de su subred, excepto para interconectar con el servidor.

```
MEDELLIN#conf term
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#access-list 111 permit ip 192.168.1.32 0.0.0.31 host
192.168.1.6
MEDELLIN(config)#int fa0/0
MEDELLIN(config-if)#ip access-group 111 in
MEDELLIN(config-if)#exit
MEDELLIN(config)#exit
MEDELLIN#
```

```
CALI#conf term
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#access-list 111 permit ip 192.168.1.64 0.0.0.31 host 192.168.1.6
CALI(config)#int fa0/0
CALI(config-if)#ip access-group 111 in
CALI(config-if)#exit
CALI(config)#exit
CALI#
```

1.13 Comprobación de la Red instalada

a. Se debe probar que la configuración de las listas de acceso fue exitosa.
b. Comprobar y Completar la siguiente tabla de condiciones de prueba para confirmar el óptimo funcionamiento de la red e.

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	Éxito
	WS_1	Router BOGOTA	Falla
	Servidor	Router CALI	Éxito
	Servidor	Router MEDELLIN	Éxito
TELNET	LAN del Router MEDELLIN	Router CALI	Falla
	LAN del Router CALI	Router CALI	Falla
	LAN del Router MEDELLIN	Router MEDELLIN	Falla
	LAN del Router CALI	Router MEDELLIN	Falla
PING	LAN del Router CALI	WS_1	Falla
	LAN del Router	WS_1	Falla

	MEDELLIN		
	LAN del Router MEDELLIN	LAN del Router CALI	Falla
PING	LAN del Router CALI	Servidor	Éxito
	LAN del Router MEDELLIN	Servidor	Éxito
	Servidor	LAN del Router MEDELLIN	Éxito
	Servidor	LAN del Router CALI	Éxito
	Router CALI	LAN del Router MEDELLIN	Falla
	Router MEDELLIN	LAN del Router CALI	Falla

2. Escenario dos

Una empresa tiene la conexión a internet en una red Ethernet, lo cual deben adaptarlo para facilitar que sus routers y las redes que incluyen puedan, por esa vía, conectarse a internet, pero empleando las direcciones de la red LAN original.

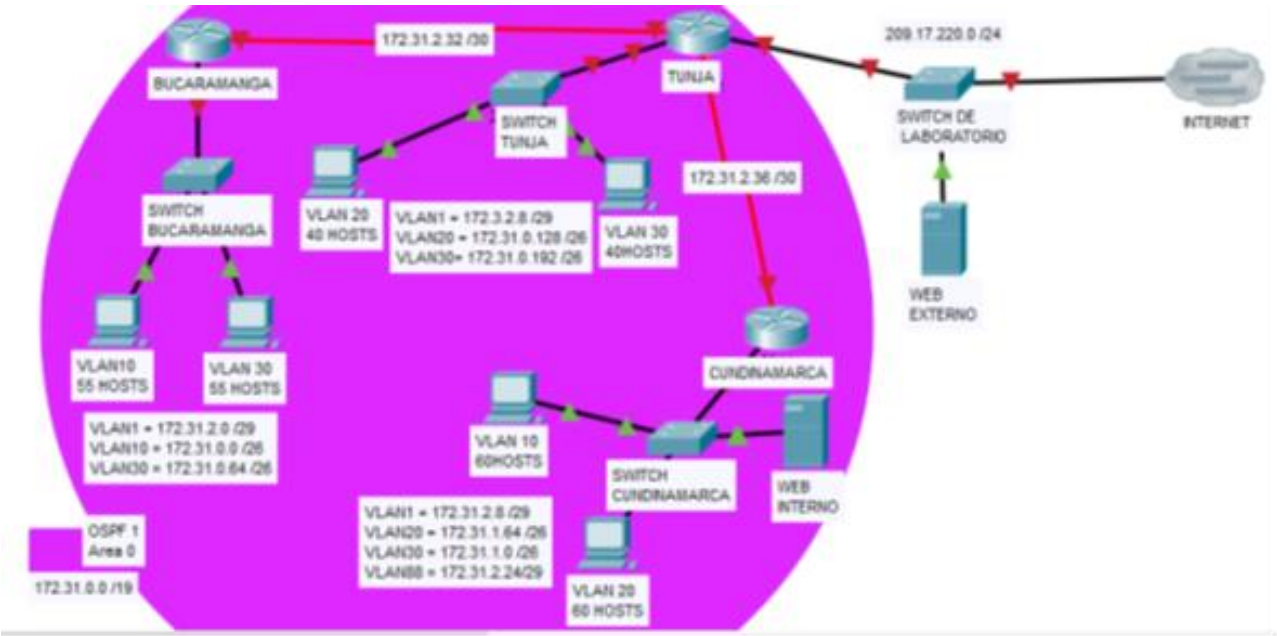

Figura 20. Imagen esquema escenario 2 propuesto

2.1 **Comprobación de la red instalada.**

Los siguientes son los requerimientos necesarios:

Todos los routers deberán tener los siguiente:
• Configuración básica.
• Autenticación local con AAA.
• Cifrado de contraseñas.
• Un máximo de internos para acceder al router.
• Máximo tiempo de acceso al detectar ataques.

2.1.1 Topologia

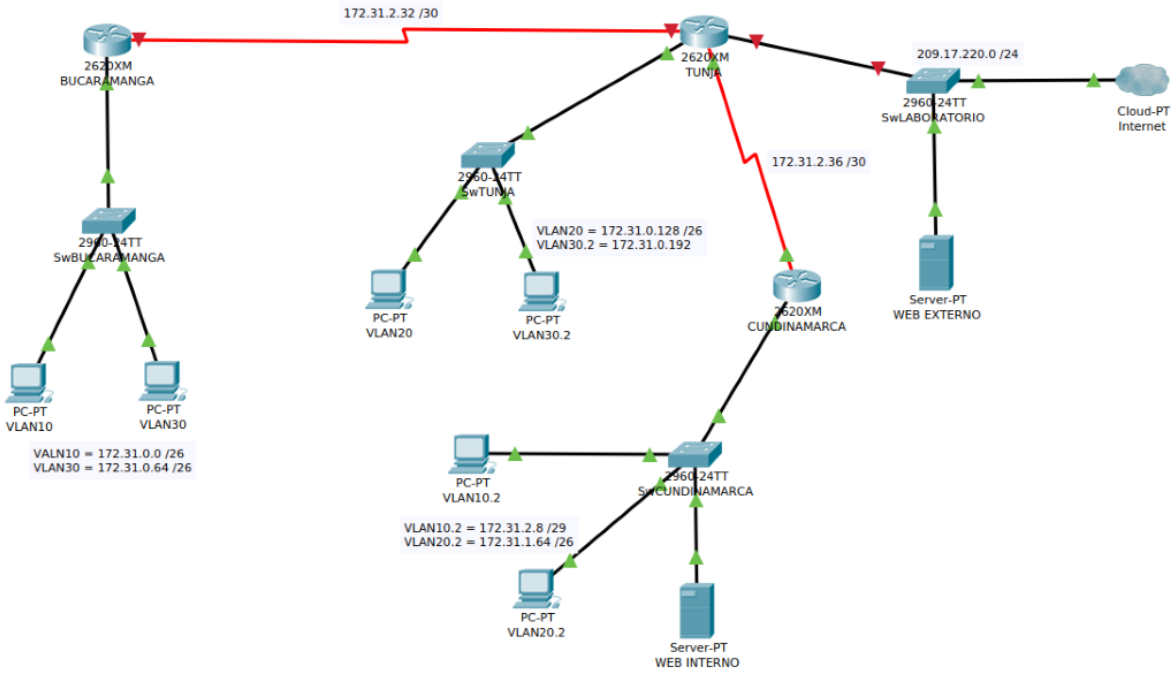

Figura 21. Imagen de esquema en Packet Tracer

2.1.2 Router Bucaramanga

```
Router>enable
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BUCARAMANGA
BUCARAMANGA(config)#no ip domain-lookup
BUCARAMANGA(config)#aaa aute
BUCARAMANGA(config)#aaa authe
BUCARAMANGA(config)#aaa authentication login local enable
BUCARAMANGA(config)#aaa new-model
BUCARAMANGA(config)#aaa authentication login AUTH local
BUCARAMANGA(config)#line console 0
BUCARAMANGA(config-line)#login authe
BUCARAMANGA(config-line)#login authentication AU
BUCARAMANGA(config-line)#login authentication AUTH
BUCARAMANGA(config-line)#line vty 0 15
BUCARAMANGA(config-line)#login authentication AUTH
BUCARAMANGA(config-line)#username cisco secret cisco
```

BUCARAMANGA(config)#exit
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
BUCARAMANGA#conf term
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#service password-encryption
BUCARAMANGA(config)#exit
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
BUCARAMANGA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
BUCARAMANGA#

2.1.3 Router Bucaramanga Interfaces y seriales

Username: cisco
Password:
BUCARAMANGA>enable
BUCARAMANGA#conf term
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#interface fastEthernet 0/0
BUCARAMANGA(config-if)#no shutdown
BUCARAMANGA(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up
BUCARAMANGA(config-if)#exit
BUCARAMANGA(config)#int se0/0
BUCARAMANGA(config-if)#ip add 172.31.2.33 255.255.255.252
BUCARAMANGA(config-if)#exit
BUCARAMANGA(config)#ip route 172.31.0.192 255.255.255.192 172.31.2.34
BUCARAMANGA(config)#ip route 172.31.0.128 255.255.255.192 172.31.2.34
BUCARAMANGA(config)#ip route 172.31.2.8 255.255.255.248 172.31.2.34
BUCARAMANGA(config)#ip route 172.31.1.64 255.255.255.192 172.31.2.34
BUCARAMANGA(config)#exit
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
BUCARAMANGA#

2.1.4 Switch Bucaramanga

Switch>enable
Switch#conf term

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SwBUCARAMANGA
SwBUCARAMANGA(config)#enable secret cisco
SwBUCARAMANGA(config)#line console 0
SwBUCARAMANGA(config-line)#password cisco
SwBUCARAMANGA(config-line)#login
SwBUCARAMANGA(config-line)#line vty 0 15
SwBUCARAMANGA(config-line)#password cisco
SwBUCARAMANGA(config-line)#login
SwBUCARAMANGA(config-line)#exit
SwBUCARAMANGA(config)#service password-encryption
SwBUCARAMANGA(config)#no ip domain-lookup
SwBUCARAMANGA(config)#do write
Building configuration...
[OK]
SwBUCARAMANGA(config)#exit
SwBUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
SwBUCARAMANGA#

2.1.5 Switch Bucaramanga Vlan

SwBUCARAMANGA#conf term
Enter configuration commands, one per line. End with CNTL/Z.
SwBUCARAMANGA(config)#vlan ?
<1-4094> ISL VLAN IDs 1-1005
SwBUCARAMANGA(config)#vlan 10
SwBUCARAMANGA(config-vlan)#vlan 30
SwBUCARAMANGA(config-vlan)#exit
SwBUCARAMANGA(config)#interface vlan10
SwBUCARAMANGA(config-if)#exit
SwBUCARAMANGA(config)#interface vlan30
SwBUCARAMANGA(config-if)#exit
SwBUCARAMANGA(config)#interface fa0/1
SwBUCARAMANGA(config-if)#switchport mode access
SwBUCARAMANGA(config-if)#switchport access vlan 10
SwBUCARAMANGA(config-if)#
SwBUCARAMANGA(config-if)#no shutdown
SwBUCARAMANGA(config-if)#exit
SwBUCARAMANGA(config)#interface fa0/2
SwBUCARAMANGA(config-if)#switchport mode access
SwBUCARAMANGA(config-if)#switchport access vlan 30
SwBUCARAMANGA(config-if)#
SwBUCARAMANGA(config-if)#no shutdown
SwBUCARAMANGA(config-if)#do write

Building configuration...
[OK]
SwBUCARAMANGA(config-if)#exit
SwBUCARAMANGA(config)#int fa0/3
SwBUCARAMANGA(config-if)#switchport mode trunk
SwBUCARAMANGA(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/3, changed state to down
SwBUCARAMANGA(config-if)#switchport trunk native vlan 1
SwBUCARAMANGA(config-if)#exit
SwBUCARAMANGA(config)#exit
SwBUCARAMANGA#

2.1.6 Router Tunja

Router>enable
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname TUNJA
TUNJA(config)#no ip domain-lookup
TUNJA(config)#aaa authentication login local enable
% Invalid input detected --- aaa not enabled
TUNJA(config)#aaa new-model
TUNJA(config)#aaa authentication login AUTH local
TUNJA(config)#line console 0
TUNJA(config-line)#login authentication AUTH
TUNJA(config-line)#line vty 0 15
TUNJA(config-line)#login authentication AUTH
TUNJA(config-line)#username cisco secret cisco
TUNJA(config)#service password-encryption
TUNJA(config)#exit
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console
TUNJA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
TUNJA#

2.1.7 Router Tunja Interfaces y seriales

TUNJA#conf term
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#interface serial 0/0
TUNJA(config-if)#ip address 172.31.2.34 255.255.255.252
TUNJA(config-if)#Ip ospf message-digest-key 1 md5 7 network
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0, changed state to down
TUNJA(config-if)#exit
TUNJA(config)#int fa0/0
TUNJA(config-if)#no shutdown
TUNJA(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up
TUNA(config-if)#exit
TUNJA(config)#int se0/1
TUNJA(config-if)#ip add 172.31.2.37 255.255.255.252
TUNJA(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1, changed state to down
TUNJA(config-if)#exit
TUNJA(config)#ip route 172.31.0.64 255.255.255.192 172.31.2.33
TUNJA(config)#ip route 172.31.0.0 255.255.255.192 172.31.2.33
TUNJA(config)#ip route 172.31.2.8 255.255.255.248 172.31.2.38
TUNJA(config)#ip route 172.31.1.64 255.255.255.192 172.31.2.38
TUNJA(config)#ip route 172.31.2.24 255.255.255.248 172.31.2.38
TUNJA(config)#exit
TUNJA#

2.1.8 Switch Tunja

Switch>enable
Switch#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SwTUNJA
SwTUNJA(config)#enable secret cisco
SwTUNJA(config)#line console 0
SwTUNJA(config-line)#password cisco
SwTUNJA(config-line)#login
SwTUNJA(config-line)#line vty 0 15
SwTUNJA(config-line)#password cisco

SwTUNJA(config-line)#login
SwTUNJA(config-line)#exit
SwTUNJA(config)#service password-encryption
SwTUNJA(config)#no ip domain-lookup
SwTUNJA(config)#do write
Building configuration...
[OK]
SwTUNJA(config)#

2.1.8 Switch Tunja Vlan

SwTUNJA#conf term
Enter configuration commands, one per line. End with CNTL/Z.
SwTUNJA(config)#vlan 20
SwTUNJA(config-vlan)#vlan 30
SwTUNJA(config-vlan)#exit
SwTUNJA(config)#interface vlan 20
SwTUNJA(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

SwTUNJA(config-if)#interface vlan 30
SwTUNJA(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up
SwTUNJA(config-if)#interface fa0/01
SwTUNJA(config-if)#switchport mode access
SwTUNJA(config-if)#switchport access vlan 20
SwTUNJA(config-if)#
SwTUNJA(config-if)#no shutdown
SwTUNJA(config-if)#exit
SwTUNJA(config)#interface fa0/2
SwTUNJA(config-if)#switchport mode access
SwTUNJA(config-if)#switchport access vlan 30
SwTUNJA(config-if)#
SwTUNJA(config-if)#no shutdown
SwTUNJA(config-if)#do write
Building configuration...
[OK]
SwTUNJA(config-if)#int fa0/3
SwTUNJA(config-if)#switchport mode trunk
SwTUNJA(config-if)#
SwTUNJA(config-if)#switchport trunk native vlan 1
SwTUNJA(config-if)#exit
SwTUNJA(config)#exit
SwTUNJA#

2.1.9 Router Cundinamaca

Router>enable
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname CUNDINAMARCA
CUNDINAMARCA(config)#no ip domain-lookup
CUNDINAMARCA(config)#aaa authentication login local enable
% Invalid input detected --- aaa not enabled
CUNDINAMARCA(config)#aaa new-model
CUNDINAMARCA(config)#aaa authentication login AUTH local
CUNDINAMARCA(config)#line console 0
CUNDINAMARCA(config-line)#login authentication AUTH
CUNDINAMARCA(config-line)#line vty 0 15
CUNDINAMARCA(config-line)#login authentication AUTH
CUNDINAMARCA(config-line)#username cisco secret cisco
CUNDINAMARCA(config)#service password-encryption
CUNDINAMARCA(config)#exit
CUNDINAMARCA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
CUNDINAMARCA#

2.1.10 Router Cundinamarca Interfaces y seriales

CUNDINAMARCA#conf term
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#int se0/0
CUNDINAMARCA(config-if)#ip add 172.31.2.38 255.255.255.252
CUNDINAMARCA(config-if)#no shutdown
CUNDINAMARCA(config-if)#
%LINK-5-CHANGED: Interface Serial0/0, changed state to up
CUNDINAMARCA(config-if)#exit
CUNDINAMARCA(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0, changed state to up
CUNDINAMARCA(config)#int fa0/0
CUNDINAMARCA(config-if)#no shutdown
CUNDINAMARCA(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up
CUNDINAMARCA(config-if)#exit
CUNDINAMARCA(config)#ip route 172.31.0.128 255.255.255.192 172.31.2.37
CUNDINAMARCA(config)#ip route 172.31.0.192 255.255.255.192 172.31.2.37
CUNDINAMARCA(config)#ip route 172.31.0.0 255.255.255.192 172.31.2.37
CUNDINAMARCA(config)#ip route 172.31.0.64 255.255.255.192 172.31.2.37
CUNDINAMARCA(config)#exit
CUNDINAMARCA#

2.1.11 Switch Cundinamarca

Switch>enable
Switch#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SwCUNDINAMARCA
SwCUNDINAMARCA(config)#enable secret cisco
SwCUNDINAMARCA(config)#line console 0
SwCUNDINAMARCA(config-line)#password cisco
SwCUNDINAMARCA(config-line)#login
SwCUNDINAMARCA(config-line)#line vty 0 15
SwCUNDINAMARCA(config-line)#password cisco
SwCUNDINAMARCA(config-line)#login
SwCUNDINAMARCA(config-line)#exit
SwCUNDINAMARCA(config)#service password-encryption
SwCUNDINAMARCA(config)#no ip domain-lookup
SwCUNDINAMARCA(config)#do write
Building configuration...
[OK]
SwCUNDINAMARCA(config)#exit
SwCUNDINAMARCA#

2.1.12 Switch Cundinamarca Vlan

SwCUNDINAMARCA#conf term
Enter configuration commands, one per line. End with CNTL/Z.
SwCUNDINAMARCA(config)#vlan 10
SwCUNDINAMARCA(config-vlan)#exit
SwCUNDINAMARCA(config)#vlan 20
SwCUNDINAMARCA(config-vlan)#exit
SwCUNDINAMARCA(config)#vlan 88
SwCUNDINAMARCA(config-vlan)#exit
SwCUNDINAMARCA(config)#int vlan 10
SwCUNDINAMARCA(config-if)#

%LINK-5-CHANGED: Interface Vlan10, changed state to up
SwCUNDINAMARCA(config-if)#int vlan 20
SwCUNDINAMARCA(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up
SwCUNDINAMARCA(config-if)#exit
SwCUNDINAMARCA(config)#vlan 88
SwCUNDINAMARCA(config-vlan)#exit
SwCUNDINAMARCA(config)#int fa0/1
SwCUNDINAMARCA(config-if)#switchport mode access
SwCUNDINAMARCA(config-if)#switchport access vlan 10
SwCUNDINAMARCA(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
Vlan10, changed state to up
SwCUNDINAMARCA(config-if)#no shutdown
SwCUNDINAMARCA(config-if)#exit
SwCUNDINAMARCA(config)#int fa0/2
SwCUNDINAMARCA(config-if)#switchport mode access
SwCUNDINAMARCA(config-if)#switchport access vlan 20
SwCUNDINAMARCA(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
Vlan20, changed state to up
SwCUNDINAMARCA(config-if)#no shutdown
SwCUNDINAMARCA(config-if)#exit
SwCUNDINAMARCA(config)#int fa0/3
SwCUNDINAMARCA(config-if)#switchport mode access
SwCUNDINAMARCA(config-if)#switchport access vlan 88
SwCUNDINAMARCA(config-if)#no shutdown
SwCUNDINAMARCA(config-if)#exit
SwCUNDINAMARCA(config)#int fa0/4
SwCUNDINAMARCA(config-if)#switchport mode trunk
SwCUNDINAMARCA(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/4, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/4, changed state to up
SwCUNDINAMARCA(config-if)#switchport trunk native vlan 1
SwCUNDINAMARCA(config-if)#exit
SwCUNDINAMARCA(config)#do write
Building configuration...
[OK]
SwCUNDINAMARCA(config)#exit
SwCUNDINAMARCA#

2.2 Servidor TFTP

Establezca un servidor TFTP y almacene todos los archivos necesarios de los routers.

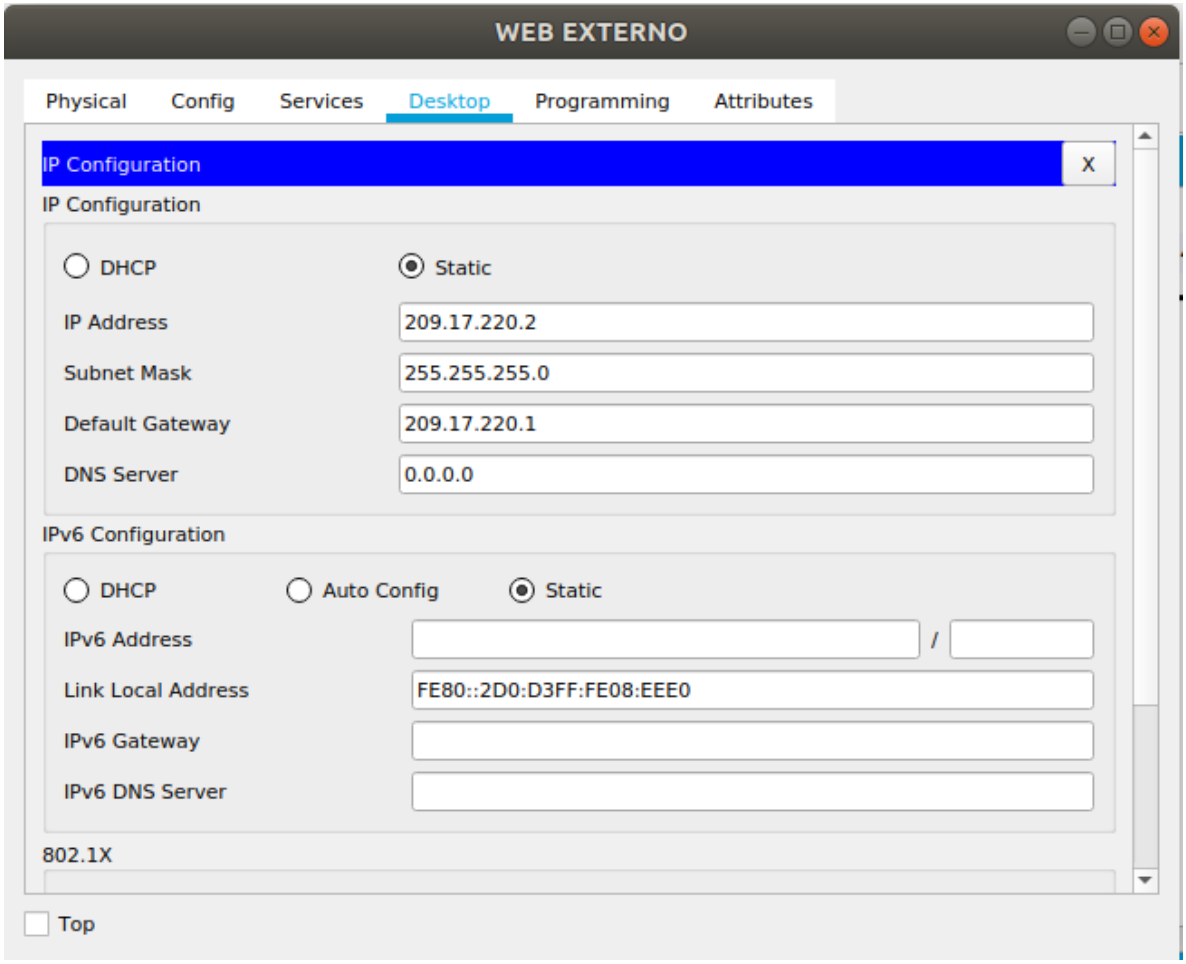

Figura 22. Imagen servidor TFTP

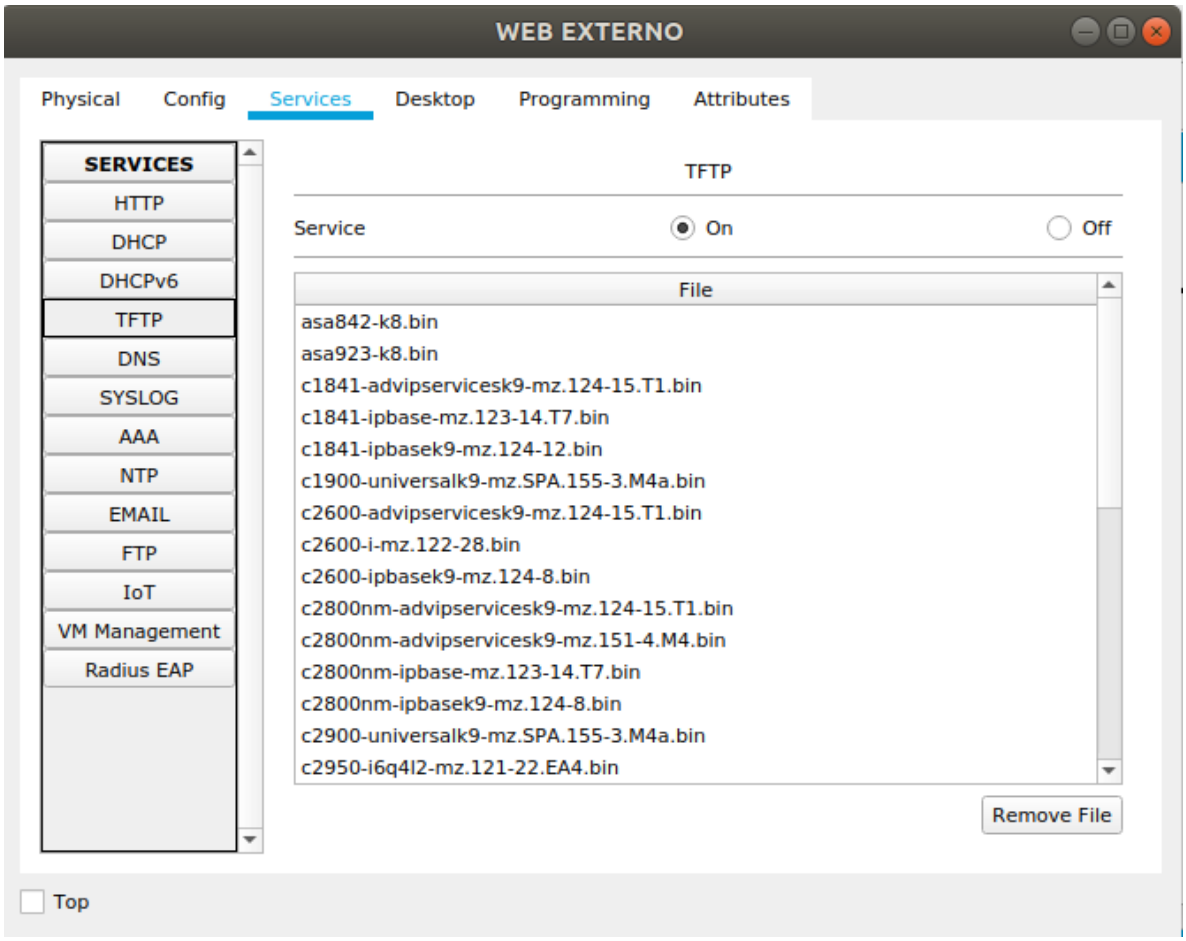

Figura 23. Imagen servidor TFTP

2.3 Servicio DHCP en los routers

El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y Cundinamarca

2.3.1 Router Bucaramanga

```
 Username: cisco
Password:
BUCARAMANGA>enable
BUCARAMANGA#conf term
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#ip dhcp pool upvn10
BUCARAMANGA(dhcp-config)#network 172.31.0.0 255.255.255.192
BUCARAMANGA(dhcp-config)#default-router 172.31.0.1
BUCARAMANGA(dhcp-config)#option 150 ip 172.31.0.1
BUCARAMANGA(dhcp-config)#exit
BUCARAMANGA(config)#ip dhcp pool upvn30
BUCARAMANGA(dhcp-config)#network 172.31.0.64 255.255.255.192
BUCARAMANGA(dhcp-config)#default-router 172.31.0.65
BUCARAMANGA(dhcp-config)#option 150 ip 172.31.0.65
BUCARAMANGA(dhcp-config)#exit
BUCARAMANGA(config)#interface fa0/0.10
BUCARAMANGA(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0.10, changed state to up
BUCARAMANGA(config-subif)#encapsulation dot1q 10
BUCARAMANGA(config-subif)#ip add 172.31.0.1 255.255.255.192
BUCARAMANGA(config-subif)#exit
BUCARAMANGA(config)#interface fa0/0.30
BUCARAMANGA(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0.30, changed state to up
BUCARAMANGA(config-subif)#encapsulation dot1q 30
BUCARAMANGA(config-subif)#ip add 172.31.0.65 255.255.255.192
BUCARAMANGA(config-subif)#exit
BUCARAMANGA(config)#router ospf 1
BUCARAMANGA(config-router)#network 172.31.0.0 0.0.0.255 area 0
BUCARAMANGA(config-router)#router-id 1.1.1.1
BUCARAMANGA(config-router)#Reload or use "clear ip ospf process" command,
for this to take effect
BUCARAMANGA(config-router)#exit
BUCARAMANGA(config)#exit
BUCARAMANGA#
```

2.3.2 Router Cundinamarca

```
Username: cisco
Password:
CUNDINAMARCA>enable
CUNDINAMARCA#conf term
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#ip dhcp pool upvn10
CUNDINAMARCA(dhcp-config)#network 172.31.2.8 255.255.255.248
CUNDINAMARCA(dhcp-config)#default-router 172.31.2.9
CUNDINAMARCA(dhcp-config)#option 150 ip 172.31.2.9
CUNDINAMARCA(dhcp-config)#exit
CUNDINAMARCA(config)#ip dhcp pool upvn20
CUNDINAMARCA(dhcp-config)#network 172.31.1.64 255.255.255.192
CUNDINAMARCA(dhcp-config)#default-router 172.31.1.65
CUNDINAMARCA(dhcp-config)#option 150 ip 172.31.1.65
CUNDINAMARCA(dhcp-config)#exit
CUNDINAMARCA(config)#interface fa0/0.10
CUNDINAMARCA(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0.10, changed state to up
CUNDINAMARCA(config-subif)#encapsulation dot1q 10
CUNDINAMARCA(config-subif)#ip add 172.31.2.9 255.255.255.248
CUNDINAMARCA(config-subif)#exit
CUNDINAMARCA(config)#interface fa0/0.20
CUNDINAMARCA(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0.20, changed state to up
CUNDINAMARCA(config-subif)#encapsulation dot1q 20
CUNDINAMARCA(config-subif)#ip add 172.31.1.65 255.255.255.192
CUNDINAMARCA(config-subif)#exit
CUNDINAMARCA(config)#int fa0/0.88
CUNDINAMARCA(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.88, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0.88, changed state to up
CUNDINAMARCA(config-subif)#encapsulation dot1q 88
CUNDINAMARCA(config-subif)#ip address 172.31.2.25 255.255.255.248
CUNDINAMARCA(config-subif)#exit
CUNDINAMARCA(config)#router ospf 1
CUNDINAMARCA(config-router)#network 172.31.1.0 0.0.0.255 area 0
CUNDINAMARCA(config-router)#network 172.31.2.0 0.0.0.255 area 0
CUNDINAMARCA(config-router)#router-id 1.1.1.1
```

CUNDINAMARCA(config-router)#Reload or use "clear ip ospf process" command, for this to take effect
CUNDINAMARCA(config-router)#exit
CUNDINAMARCA(config)#exit
CUNDINAMARCA#

2.4 NAT

El web server deberá tener NAT estático y el resto de los equipos de la topología emplearan NAT de sobrecarga (PAT).

Username: cisco
Password:
TUNJA>enable
TUNJA#conf term
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#ip nat inside source static 172.31.2.28 209.165.220.4
TUNJA(config)#access-list 1 permit 172.0.0.0 0.255.255.255
TUNJA(config)#ip nat inside source list 1 interface fa1/0 overload
TUNJA(config)#int fa1/0
TUNJA(config-if)#ip nat outside
TUNJA(config-if)#int f0/0.20
TUNJA(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0.20, changed state to up
TUNJA(config-subif)#ip nat inside
TUNJA(config-subif)#int f0/0.30
TUNJA(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0.30, changed state to up
TUNJA(config-subif)#ip nat inside
TUNJA(config-subif)#int se0/0
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#int se0/1
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#exit
TUNJA(config)#ip route 0.0.0.0 0.0.0.0 209.165.220.3
TUNJA(config)#router ospf 1
TUNJA(config-router)#default-information originate
TUNJA(config-router)#exit
TUNJA(config)#exit
TUNJA#

2.4 Enrutamiento autenticación

El enrutamiento deberá tener autenticación.

BUCARAMANGA#conf term
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#int se0/0
BUCARAMANGA(config-if)#ip ospf authentication message-digest
BUCARAMANGA(config-if)#ip ospf message-digest-key 1 md5 cisco
BUCARAMANGA(config-if)#exit
BUCARAMANGA(config)#exit
BUCARAMANGA#

CUNDINAMARCA#conf term
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#int se0/0
CUNDINAMARCA(config-if)#ip ospf authentication message-digest
CUNDINAMARCA(config-if)#ip ospf message-digest-key 1 md5 cisco
CUNDINAMARCA(config-if)#exit
CUNDINAMARCA(config)#exit
CUNDINAMARCA#

TUNJA#conf term
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#int se0/0
TUNJA(config-if)#ip ospf authentication message-digest
TUNJA(config-if)#ip ospf message-digest-key 1 md5 cisco
OSPF: Key 1 already exists
TUNJA(config-if)#int se0/1
TUNJA(config-if)#ip ospf authentication message-digest
TUNJA(config-if)#ip ospf message-digest-key 1 md5 cisco
TUNJA(config-if)#exit
TUNJA(config)#exit
TUNJA#

2.5 Listas de control de acceso:

Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.

```
CUNDINAMARCA>enable
CUNDINAMARCA#conf term
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#int se0/0
CUNDINAMARCA(config-if)#access-list 111 deny ip 172.31.1.64 0.0.0.63
209.165.220.0 0.0.0.255
CUNDINAMARCA(config)#access-list 111 permit ip any any
CUNDINAMARCA(config)#int f0/0.20
CUNDINAMARCA(config-subif)#exit
```

Los hosts de VLAN 10 en Cundinamarca si acceden a internet y no a la red interna de Tunja.

```
CUNDINAMARCA(config)#access-list 112 permit ip 172.31.1.0 0.0.0.63
209.165.220.0 0.0.0.255
CUNDINAMARCA(config)#access-list 112 deny ip any any
CUNDINAMARCA(config)#int f0/0.10
CUNDINAMARCA(config-subif)#ip access-group 112 in
CUNDINAMARCA(config-subif)#exit
CUNDINAMARCA(config)#exit
CUNDINAMARCA#
```

Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet.

```
TUNJA#conf term
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#access-list 111 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0
0.0.0.255 eq 80
TUNJA(config)#access-list 111 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0
0.0.0.255 eq 21
TUNJA(config)#access-list 111 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0
0.0.0.255 eq 20
TUNJA(config)#int f0/0.30
TUNJA(config-subif)#ip access-group 111 in
TUNJA(config-subif)#exit
```

Los hosts de VLAN 20 en Tunja solo acceden a la VLAN 20 de Cundinamarca y VLAN 10 de Bucaramanga.

```
TUNJA(config)#access-list 112 permit ip 172.31.0.128 0.0.0.63 172.31.1.64
0.0.0.63
TUNJA(config)#access-list 112 permit ip 172.31.0.128 0.0.0.63 172.31.0.0
0.0.0.63
TUNJA(config)#int f0/0.20
TUNJA(config-subif)#ip access-group 112 in
TUNJA(config-subif)#exit
TUNJA(config)#exit
TUNJA#
```

Los hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10.

```
BUCARAMANGA>enable
BUCARAMANGA#conf term
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#access-list 111 permit ip 172.31.0.64 0.0.0.63
209.165.220.0 0.0.0.255
BUCARAMANGA(config)#int f0/0.30
BUCARAMANGA(config-subif)#ip access-group 111 in
BUCARAMANGA(config-subif)#exit
```

Los hosts de VLAN 10 en Bucaramanga acceden a red de Cundinamarca (VLAN 20) y Tunja (VLAN 20), no internet.

```
BUCARAMANGA(config)#access-list 112 permit ip 172.31.0.0 0.0.0.63
172.31.1.64 0.0.0.63
BUCARAMANGA(config)#access-list 112 permit ip 172.31.0.0 0.0.0.63
172.31.0.128 0.0.0.63
BUCARAMANGA(config)#int f0/0.10
BUCARAMANGA(config-subif)#ip access-group 112 in
BUCARAMANGA(config-subif)#exit
```

Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.

```
BUCARAMANGA(config)#access-list 113 deny ip 172.31.2.0 0.0.0.7 172.31.0.0
0.0.0.63
BUCARAMANGA(config)#access-list 113 deny ip 172.31.0.64 0.0.0.63 172.31.0.0
0.0.0.63
BUCARAMANGA(config)#access-list 113 permit ip any any
BUCARAMANGA(config)#int f0/0.10
BUCARAMANGA(config-subif)#ip access-group 113 out
BUCARAMANGA(config-subif)#exit
BUCARAMANGA(config)#exit
BUCARAMANGA#


CUNDINAMARCA>enable
CUNDINAMARCA#conf term
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#access-list 113 deny ip 172.31.2.8 0.0.0.7 172.31.1.64
0.0.0.63
CUNDINAMARCA(config)#access-list 113 deny ip 172.31.1.0 0.0.0.63 172.31.1.64
0.0.0.63
CUNDINAMARCA(config)#access-list 113 deny ip 172.31.2.24 0.0.0.7 172.31.1.64
0.0.0.63
CUNDINAMARCA(config)#access-list 113 permit ip any any
CUNDINAMARCA(config)#int f0/0.20
CUNDINAMARCA(config-subif)#ip access-group 113 out
CUNDINAMARCA(config-subif)#exit
CUNDINAMARCA(config)#


TUNJA#conf term
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#access-list 113 deny ip 172.3.2.8 0.0.0.7 172.31.0.128 0.0.0.63
TUNJA(config)#access-list 113 deny ip 172.3.0.192 0.0.0.63 172.31.0.128
0.0.0.63
TUNJA(config)#access-list 113 permit ip any any
TUNJA(config)#int f0/0.20
TUNJA(config-subif)#ip access-group 113 out
TUNJA(config-subif)#exit
TUNJA(config)#
```

Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen
accedo a los routers e internet.

```
BUCARAMANGA>enable
BUCARAMANGA#conf term
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#access-list 3 permit 172.31.2.0 0.0.0.7
BUCARAMANGA(config)#access-list 3 permit 172.3.2.8 0.0.0.7
BUCARAMANGA(config)#access-list 3 permit 172.31.2.8 0.0.0.7
BUCARAMANGA(config)#line vty 0 15
BUCARAMANGA(config-line)#access-class 3 in
BUCARAMANGA(config-line)#exit
BUCARAMANGA(config)#exit
BUCARAMANGA#
```

```
CUNDINAMARCA#conf term
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#access-list 3 permit 172.31.2.0 0.0.0.7
CUNDINAMARCA(config)#access-list 3 permit 172.3.2.8 0.0.0.7
CUNDINAMARCA(config)#access-list 3 permit 172.31.2.8 0.0.0.7
CUNDINAMARCA(config)#line vty 0 15
CUNDINAMARCA(config-line)#access-class 3 in
CUNDINAMARCA(config-line)#exit
CUNDINAMARCA(config)#
```

```
TUNJA(config)#access-list 3 permit 172.31.2.0 0.0.0.7
TUNJA(config)#access-list 3 permit 172.3.2.8 0.0.0.7
TUNJA(config)#access-list 3 permit 172.31.2.8 0.0.0.7
TUNJA(config)#line vty 0 15
TUNJA(config-line)#access-class 3 in
TUNJA(config-line)#exit
TUNJA(config)#
```

Conclusiones

Como hemos visto el curso de profundización CISCO comprende una temática específica y general sobre fundamentos en las telecomunicaciones; lo que representa un gran avance dentro de mi campo de formación profesional.

Dentro del desarrollo de este trabajo final para el diplomado pusimos en práctica muchos de los conceptos que desarrollamos en los trabajos colaborativos de las fases anteriores, se implementaron dos escenarios en los cuales se administró de forma correcta toda una red para una empresa.

Podemos decir que aprendimos a realizar configuraciones básicas en equipos Cisco, configurar diferentes dispositivos y realizar la simulación con múltiples opciones de análisis

Bibliografía

Globales. (2018). *https://sites.google.com/*. Obtenido de https://sites.google.com/site/redeslocalesyglobales/4-configuracion-de-red/4-redes-de-area-local-virtuales-vlans/5-configuracion-de-vlans-basadas-en-la-configuracion-de-puertos

Lucas, M. W. (2009). *https://onedrive.live.com/*. Obtenido de https://onedrive.live.com/?authkey=%21APvgFndukyJdHHQ&cid=483D35BEE8610962&id=483D35BEE8610962%213570&parId=483D35BEE8610962%213568&o=OneUp

Macfarlane, J. (2006). *Network Routing Basics.* Indianapolis: Wiley Publishing.

Todos, R. d. (30 de Marzo de 2016). *https://www.youtube.com/*. Obtenido de https://www.youtube.com/watch?v=vdiGOFwJiP4